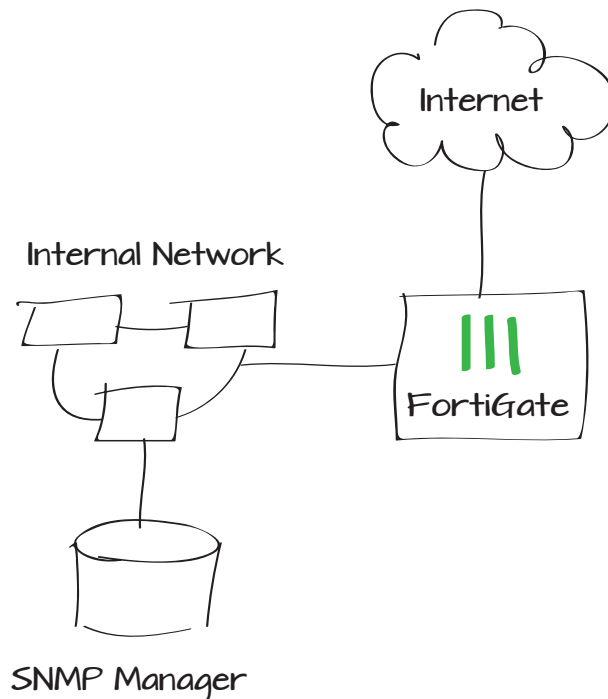


Using SNMP to monitor the FortiGate unit

The Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers.

In this example, you configure the FortiGate SNMP agent and an example SNMP manager so that the SNMP manager can get status information from the FortiGate unit and so that the FortiGate unit can send traps to the SNMP manager.

1. Configuring the FortiGate SNMP agent
2. Enabling SNMP on a FortiGate interface
3. Downloading Fortinet MIB files to and configuring an example SNMP manager
4. Results



Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**.

Configure the SNMP agent.

SNMP Agent

☒ Enable

Description

Company FortiGate unit

Location

Head Office, server room

Contact

admin@company.com

Apply

SNMP v1/v2c

Create New

Edit

Delete

	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	FortiGates	✓	✓	<input checked="" type="checkbox"/>

SNMP v3

Create New

Edit

Delete

	User Name	Security Level	Notification Host	Queries
--	-----------	----------------	-------------------	---------

- FortiGate SNMP MIB
- Download FortiGate MIB File

Download Fortinet Core MIB File

Under **SNMP v1/v2c** create a new community.

Add the IP address of SNMP manager (in the example, 192.168.1.114/32). If required, change the query and trap ports to match the SNMP manager.

You can add multiple SNMP managers or set the IP address/Netmask to 0.0.0.0/0.0.0.0 and the Interface to ANY so that any SNMP manager on any network connected to the FortiGate unit can use this SNMP community and receive traps from the FortiGate unit.

Enable the **SNMP Events** (traps) that you need. In most cases leave them all enabled.

Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces**.

Enable SNMP administrative access on the interface connected to the same network as the SNMP manager.

Edit SNMP Community

Community NameFortiGates

Hosts:

IP Address/Netmask	Interface	Delete
192.168.1.114/255.255.255.255	port1	

Add

Queries:

Protocol	Port	Enable
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>

Traps:

Protocol	Local	Remote	Enable
v1	162	162	<input checked="" type="checkbox"/>
v2c	162	162	<input checked="" type="checkbox"/>

SNMP Events

☒ CPU usage is high

☒ Log disk space is low

☒ VPN tunnel up

☒ WiFi Controller AP up

☒ FortiSwitch Controller Session up

☒ HA cluster status is changed

☒ HA member up

☒ Virus detected

☒ Fragmented email detected

☒ Oversized file/email blocked

☒ AV bypass happens

☒ IPS anomaly detected

☒ IPS package updated

☒ System enters conserve mode

☒ FortiAnalyzer disconnected

☒ Memory is low

☒ Interface IP is changed

☒ VPN tunnel down

☒ WiFi Controller AP down

☒ FortiSwitch Controller Session down

☒ HA heartbeat failure

☒ HA member down

☒ Matched file pattern detected

☒ Oversized file/email detected

☒ Oversized file/email passed

☒ IPS attack detected

☒ System configuration is changed

Nameport1 (00:09:0F:4E:10:1F)

Alias

Link StatusUp

Addressing mode

☒ Manual

☐ DHCP

☐ Dedicate to FortiAP/FortiSwitch

IP/Network Mask:192.168.1.99/255.255.255.0

IPv6 Address:::/0

Administrative Access

☒ HTTPS

☒ SSH

☒ PING

☒ SNMP

☐ HTTP

☐ TELNET

☐ FMG-Access

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ SSH

☐ PING

☐ SNMP

☐ HTTP

☐ TELNET

☐ FMG-Access

Downloading the Fortinet MIB files to and configuring an example SNMP manager

Go to **System > Config > SNMP** to download FortiGate SNMP MIB file and the Fortinet Core MIB file.

Two types of MIB files are available for FortiGate units: the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields, and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields, and information that is specific to FortiGate units.

Configure the SNMP manager at 192.168.1.114 to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs.

Results

This example uses the SolarWinds SNMP trap viewer.

In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.

SNMP Agent

☒ Enable

Description

Company FortiGate unit

Location

Head Office, server room

Contact

admin@company.com

Apply

SNMP v1/v2c

Create New Edit Delete

	Community Name	Queries	Traps	Enable
	FortiGates	✓	✓	<input checked="" type="checkbox"/>

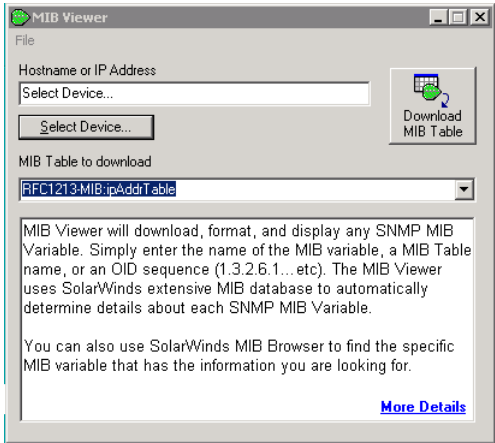
SNMP v3

Create New Edit Delete

	User Name	Security Level	Notification Host	Queries
--	-----------	----------------	-------------------	---------

FortiGate SNMP MIB

[Download FortiGate MIB File](#)
[Download Fortinet Core MIB File](#)



Choose **Select Device**, enter the IP address of the FortiGate unit, and choose the appropriate community string credentials.

Open the SNMP Trap Receiver and select **Launch**.

Device Credentials

Device or IP address:

192.168.1.99

Credentials:

☒ Community string:

FortiGates

☐ SNMP Version 3:


Select or add credentials

Test

OK

Cancel


1 search results for SNMP Trap Receiver

 **SNMP Trap Receiver**

Logs, and display SNMP traps sent from a network device, server, or application

- Receives, logs, and displays SNMP traps
- Includes traps that are sent from a network device, server or application

Launch



SNMP Trap Receiver

File Edit Traps Help

Export

Print

Clear

Pause

Settings


Trap Time	IP Address	Community	Device Type	Trap Details
-----------	------------	-----------	-------------	--------------

On the FortiGate unit, perform an action to trigger a trap (for example, change the IP address of the DMZ interface).

Verify that the SNMP manager receives the trap.

On the FortiGate unit, view log messages showing the trap was sent by going to **Log & Report > Event Log > System**.

Trap Time	IP Address	Community	Device Type	Trap Details
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapInfg.1.3.0.201 fnTrapInfg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.201 fnTrapInfg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2 experimental.1057.1 = 192.168.1.99
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.6.0.1004 fnTrapInfg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.1004 fnTrapInfg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0 experimental.1057.1 = 192.168.1.99

cfgpath	system.interface	Date/Time	10:49:28 (Fri Mar 8 10:49:28 2013)
Virtual Domain	root	Level	information 000000
Timestamp	Fri Mar 8 10:49:28 2013	cfgtid	2949201
logid	44547	Sub Type	system
User Interface	GUI(172.20.120.21)	User	 admin
Action	Edit	cfgobj	dmz
roll	65409	cfgattr	ip[10.10.10.99 255.255.255.0->10.10.10.1
Message	Edit system.interface dmz		